



Department of Homeland Security Daily Open Source Infrastructure Report for 19 November 2007

Current Nationwide



[For info click here](#)

- According to the *Associated Press*, a preliminary FAA investigation found that the near-collision of two commercial aircraft at 25,000 feet over Indiana was caused by air traffic controller error. An FAA spokeswoman said the Tuesday evening incident happened amid a shift change during a busy time at the Chicago Center radar facility in Aurora, Illinois. (See item [14](#))
- In an *Army Times* report, the Department of Veterans Affairs announced that a computer containing the names, Social Security numbers and birthdates of 12,000 veterans was taken over the Veterans' Day weekend from a VA medical center in Indianapolis. The records are of veterans who had been treated at the hospital. VA policy calls for immediate notification of those involved and the provision of free credit monitoring for those at risk of identity theft. Federal, state and local law-enforcement agencies are investigating the theft. (See item [10](#))

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical](#); [Nuclear Reactors](#); [Materials and Waste](#); [Defense Industrial Base](#); [Dams](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#); [Information Technology](#); [Communications](#); [Commercial Facilities](#)

Sustenance and Health: [Agriculture and Food](#); [Water](#); [Public Health and Healthcare](#)

Federal and State: [Government Facilities](#); [Emergency Services](#); [National Monuments and Icons](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: **Physical**: ELEVATED, **Cyber**: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *November 16, St. Cloud Times* – (Minnesota) **Oil spills into Mississippi River**. More than 220 gallons of hydraulic oil spilled into a storm drain Thursday on St. Cloud, Minnesota's East Side, and an unknown amount apparently escaped into the Mississippi

River. The spill came from a hydraulic line on a compactor at Phillips Recycling Systems. The St. Cloud police chief said authorities are investigating the break as suspicious. Police believe someone may have cut the line intentionally. They continue to investigate the incident as a possible attempted theft or act of vandalism. The hydraulic fluid is about 98 percent mineral oil and low in toxicity, said a spokesman for the Minnesota Pollution Control Agency. It would have become diluted by river water and does not pose a threat to human health or the environment.

Source:

<http://www.sctimes.com/apps/pbcs.dll/article?AID=/20071116/NEWS01/111150063/1009>

2. *November 15, Platts* – (Arizona) **FERC clears Transwestern plan to hike pipe capacity to Phoenix.** The Federal Energy Regulatory Commission (FERC) on Thursday approved a plan by Transwestern Pipeline to expand capacity into Phoenix, Arizona. To help diversify gas transportation to the fast-growing region, Transwestern plans to expand its existing interstate system in New Mexico and Arizona to transport an additional 500,000 Mcf/d to the Phoenix area. At present, the area depends solely on the El Paso Natural Gas pipeline system, which has struggled to keep up with population growth. Gas hauled by Transwestern would come out of the Rocky Mountain and San Juan basins and be used primarily for power generation around Phoenix. It also aims to increase gas supply reliability and flexibility for customers in central and southern Arizona, according to the environmental impact statement, released in September, endorsing the project.

Source:

<http://www.platts.com/Natural%20Gas/News/6596790.xml?sub=Natural%20Gas&p=Natural%20Gas/News&?undefined&undefined>

[\[Return to top\]](#)

Chemical Industry Sector

3. *November 16, Salem News* – (Massachusetts) **Feds find gaps in state chemical storage regulations.** Federal investigators of last November's chemical plant explosion in Massachusetts have found the state lacking in the way it regulates the storage and handling of hazardous materials. The state's top fire official, in turn, said it is up to towns and cities to govern the type and amount of chemicals stored in such enterprises. The U.S. Chemical Safety Board said ink manufacturer CAI Inc. and paint maker Arnel Co. used a license issued more than 60 years ago to store flammable materials. "The CAI/Arnel site was originally licensed under state law for just 250 gallons of 'lacquer' back in 1944, to a company that long since sold the property," the lead investigator said yesterday in a statement accompanying the board's updated findings. Neighbors of the plant have proposed the creation of the Danvers Hazardous Material Safety Board, a panel of residents, business owners and town officials. The advisory board, which the selectmen have yet to endorse, would review all matters related to the use and storage of hazardous materials in town, including the issuance and renewal of permits, licenses and registrations.

Source: http://www.salemnews.com/punews/local_story_320094032

4. *November 15, WCNC Charlotte* – (North Carolina) **Chemical tests planned near area plant.** State health officials want to know if chemicals from a local plant are affecting more than the people who work there. A health study will be done over the next few weeks near the Foamex LP facility in Cornelius, North Carolina. The concern is over a chemical called toluene diisocyanate, or TDI. The health department describes TDI as a chemical used to make many household products, including foam for furniture cushions, and some plastics and sealants. It is released into the environment during some manufacturing activities. Health officials know the chemical can cause health problems for workers exposed to the chemical, but they are unsure about the effects outside plants. Source: <http://www.wcnc.com/news/local/stories/wcnc-111507-ah-chemicaltests.6787fa6.html>

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

5. *November 16, Associated Press* – (New York) **Rough water forces power reduction at upstate nuclear plant.** Turbulent water on Lake Ontario is again blamed for a power reduction at one of the nuclear power plants in the Oswego area. A spokeswoman at the James A. FitzPatrick nuclear power plant says operators reduced the reactor's power capacity to 65 percent overnight as a precaution to guard against lake algae from entering the facility's water intake system. The problem had forced the shut down of the Fitzpatrick reactor three times since September. Source: <http://www.wcax.com/global/story.asp?s=7370278>
6. *November 16, Monroe News* – (Michigan) **DTE restarts Fermi after automatic shutdown.** DTE Energy restarted its Fermi 2 nuclear power plant early today after concluding that the automatic shutdown of the reactor early Thursday apparently was caused by worker error. When the shutdown occurred, "an in-plant switch inadvertently was activated as plant personnel were preparing to perform maintenance on reactor water-level instrumentation," said a DTE spokesman. Reports the utility filed with the federal Nuclear Regulatory Commission indicated that plant workers were hanging protective tags on some critical plant equipment at the time of the automatic shutdown. The Fermi reactor was operating at 9 percent of power at the time of the shutdown, but it was not generating electricity. When the reactor suddenly stopped, it had been operating for little more than 24 hours after being restarted following a 47-day shutdown for maintenance and refueling. Operators spent much of Thursday reviewing plant systems to ensure no equipment problems caused the shutdown. All plant safety systems worked as designed during the rapid shutdown. Operators restarted the plant this morning, and it was operating at very low power levels by late morning. Source: <http://www.monroenews.com/apps/pbcs.dll/article?AID=/20071116/NEWS01/111160064>
7. *November 15, Baltimore Business Journal* – (Maryland) **New reactor sought for Calvert Cliffs nuclear plant.** UniStar Nuclear Energy, a joint venture of Constellation Energy Group and the EDF Group, has filed an official application with the state to

build a new nuclear power reactor at the Calvert Cliffs nuclear plant. In June, Constellation Energy Group and the EDF Group announced a new venture and interest in building a new reactor at the Southern Maryland site. Although UniStar has not made a decision to move forward with the project, it has filed an application with the Maryland Public Service Commission, the state agency that oversees the utility industry. “A third reactor at our high-performing Calvert Cliffs site offers the potential for an economic and environmentally sound means to provide additional base-load electricity to meet anticipated growth, both regionally and within the state of Maryland,” the executive vice president of Constellation Energy and chairman of UniStar New Energy, said in a statement Thursday.

Source:

http://www.bizjournals.com/baltimore/stories/2007/11/12/daily30.html?ana=from_rss

[\[Return to top\]](#)

Defense Industrial Base Sector

8. *November 16, Mass High Tech* – (National) **KVH collects Phase 2 contract for fiber optic compass.** KVH Industries Inc. reports it has been awarded a \$730,000, Phase 2 Small Business Innovative Research grant from the Department of Defense to develop a fiber optic gyro-based compass, potentially much smaller and lighter than systems now available. The compass is intended to permit users to rapidly and precisely determine true north, which is critical for indirect fire weapons such as mortars, far target location or in situations where GPS measurements are unavailable, such as in a tunnel, deep forest, or urban canyon, according to KVH officials.

Source:

http://www.bizjournals.com/masshightech/stories/2007/11/12/daily32.html?ana=from_rss

9. *November 16, Mass High Tech* – (National) **C4 Systems selected for \$78M Army broadband deal.** General Dynamics C4 Systems Inc. has received a \$78.3 million order from the Army as part of an indefinite delivery/indefinite quantity contract worth up to \$1.4 billion for providing broadband network and satellite communications capabilities to soldiers deployed in Iraq and Afghanistan. Delivery of equipment, including networking hubs, network nodes and network management suites, is set to begin in May 2008.

Source:

http://www.bizjournals.com/masshightech/stories/2007/11/12/daily33.html?ana=from_rss

[\[Return to top\]](#)

Banking and Finance Sector

10. *November 15, Army Times* – (Indiana) **Computer with veterans' data stolen.** The Department of Veterans Affairs announced that a computer containing the names, Social Security numbers and birthdates of 12,000 veterans was taken over the Veterans' Day

weekend from the VA medical center in Indianapolis. Three computers were taken from an unlocked room, but one computer contained records that could be used for identity theft. The records are of veterans who had been treated as patients at the hospital. A policy established earlier this year calls for immediate notification of everyone whose information is missing and a review of the potential threat of identity theft in such situations. If there is a risk of identity theft, VA policy calls for the government to provide free credit monitoring to those affected. Federal, state and local law-enforcement agencies are investigating the theft.

[\[Return to top\]](#)

Transportation Sector

11. *November 16, Fox 12 Oregon* – (Oregon) **FBI: Man tried to open plane door on PDX-bound flight.** FBI agents and Port of Portland officers arrested an Illinois man Thursday night after he allegedly became unruly on a flight from Chicago to Portland, Oregon. The flight attendants told officials that the passenger became agitated after they denied him alcohol and they moved him to the rear of the plane, where he tried to open the rear door and touch a female flight attendant. Agents said the flight crew used handcuffs to restrain him for the duration of the flight. The man will appear in a federal courtroom on charges of disrupting the flight and interfering with the flight crew.
Source: <http://www.kptv.com/news/14614228/detail.html>
12. *November 16, Rocky Mountain News* – (Colorado) **Airport hostage scare a ‘young pilot’ error.** On Thursday, emergency crews raced to Centennial Airport near Denver, Colorado, after hearing there might be a hostage situation aboard a plane. It turned out to be a misunderstanding, however, stemming from “a communications error” by a young pilot. The airplane landed safely and no injuries were reported.
Source: <http://www.rockymountainnews.com/news/2007/nov/16/airport-hostage-scare-a-young-pilot-error/>
13. *November 16, Associated Press* – (Louisiana) **Natural gas well erupts, shuts down Interstate 10 both ways.** A natural gas well blew and caught fire, causing the closure of Interstate 10 in both directions at La. 415 until at least Sunday evening, Louisiana State Police said. State police learned of the rupture about 5 p.m., and several motorists reported a significant haze and a strong gas smell while traveling on the Whiskey Bay Bridge, authorities said. The gas leak happened as workers from Bridas Energy were drilling to establish a new well. In doing so, pressure built and essentially blew the line, state police said. No injuries were reported and no evacuations were ordered.
Source:
<http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20071116/BREAKINGNEWS/71116007>
14. *November 15, Associated Press* – (Indiana) **Two planes come within seconds of colliding over Indiana.** According to a preliminary investigation by the Federal

Aviation Administration (FAA), two planes came within seconds of colliding at 25,000 feet over Indiana because of an error by an air traffic controller. A FAA spokeswoman said the Tuesday evening incident happened amid a shift change during a busy time at the Chicago Center radar facility in Aurora, Illinois. Officials say that controller directed a Midwest Airlines plane flying east from Milwaukee, Wisconsin, into the path of a United Express jet heading west out of Greensboro, North Carolina.

Source: <http://www.foxnews.com/story/0,2933,311867,00.html>

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture and Food Sector

15. *November 16, Associated Press* – (National) **Contaminated sausage rolls recalled.**

Texas-based Double B Foods Incorporated is recalling about 98,000 pounds of frozen sausage roll products because of concerns that they are potentially contaminated with listeria monocytogenes, which can cause listeriosis, a rare but potentially fatal disease. The U.S. Department of Agriculture (USDA) announced the voluntary recall yesterday. The products were produced on various dates between October 25th and November 6th. The company found the potential problem during an in-plant testing program. In addition to being sold in Texas and Georgia, the products were distributed to institutions, catalog sales and distribution centers in Alabama, Arkansas, Florida, Louisiana, Mississippi, New Jersey, New Mexico, New York, Oklahoma and Pennsylvania.

Source: <http://www.wsav.com/midatlantic/sav/news.apx.-content-articles-SAV-2007-11-16-0013.html>

16. *November 16, Fox 6 San Diego* – (California) **USDA releases fruit flies to control infestation of destructive pest.** A release of sterile Mexican fruit flies began Friday in Escondido in an effort to eradicate an infestation of the pest, county agriculture officials said. The California Department of Food and Agriculture and the U.S. Department of Agriculture will release 5 million sterile Mexican fruit flies by plane each week -- through next spring -- in a nine-square-mile area. The sterile fruit flies will mate with wild fruit flies, making the insects' eggs infertile and eventually eradicating any infestation. Mexican fruit flies damage more than 50 different crops by laying eggs in fruit, which later serves as food for the larvae. The eradication program was prompted by the discovery of five female Mexican fruit flies at two locations in Escondido, according to the San Diego County Department of Agriculture, Weights and Measures. Source: http://www.fox6.com/news/local/story.aspx?content_id=8af31572-9596-429a-87dd-9dd7b8885c60

17. *November 15, Associated Press* – (National) **USDA says ConAgra's safety plan at pot**

pie plant was flawed. USDA inspectors found flaws in the safety plan ConAgra Foods Inc. used at the Missouri plant where it makes the Banquet and private label pot pies that were linked to a salmonella outbreak and recall last month. A spokeswoman for the Department of Agriculture's Food Safety and Inspection Service said Thursday that ConAgra took action to correct the problems found after the October 11 recall, so the government did not have a problem with the company's announcement Wednesday that production had been resumed at the plant in question. The company expects the pies to return to stores sometime in January. ConAgra said that while they have not identified the source of the salmonella in the pot pies, they have implemented new testing procedures at the plant and at its ingredient suppliers that should ensure safety.
Source: <http://www.bnd.com/336/story/178816.html>

[\[Return to top\]](#)

Water Sector

18. *November 16, East Valley Tribune* – (Arizona) **Water scare outrages Scottsdale residents.** Water from a south Scottsdale Superfund site laced with nearly double the maximum legal limit of a suspected cancer-causing chemical may have entered a drinking-water supply in Scottsdale, Arizona, during an eight-day period last month, federal officials revealed on November 15. The chief of the U.S. Environmental Protection Agency's Superfund Private Site Section said the incident happened at the Miller Road Treatment Facility. The facility has three treatment towers, two of which are normally in use. On October 15, workers at the site shut down one of the towers for inspection and shifted operations to the third, unused tower. Samples were taken of the water leaving the new tower and sent off to a lab. The EPA did not receive the results from tests on the water, however, until Wednesday. That is because the first lab had equipment problems, requiring that the sample be sent to a second lab. The EPA then notified the public within the seven days required by its own guidelines for the Scottsdale Superfund site. During the tower's eight days of operation, the tainted water was sent to a facility run by Arizona American Water Co. -- a private water utility -- where it was blended with water from several other sources before being sent to customers. Company representatives asserted that in the blending, the TCE was diluted to within federal guidelines. The EPA is investigating how the water may have been tainted. "Based on what the company has told us, we do not believe anyone was exposed to levels of concern," the chief of the EPA's Superfund Private Site Section said. At the same meeting, representatives of the EPA also said they have rejected Motorola's request to remove air filters at the Scottsdale Central Groundwater Treatment Facility, which treats contaminated groundwater from the North Indian Bend Wash Superfund site. Doing so would have put about 6 pounds of a solvent called trichloroethylene, or TCE, into the air each day in an area bordered by residential neighborhoods, according to Motorola representatives.
Source: <http://www.eastvalleytribune.com/story/102133>

19. *November 15, Hattiesburg American* – (Mississippi) **Boil-water notice issued for Willow Grove.** The Mississippi State Department of Health is issuing a boil water alert for customers who receive their drinking water from the Willow Grove Water

Association water supply located in Covington County. Water system officials notified the Department of Health of pressure loss due to a leak on a water line. Customers will be notified when tests show that the water is safe to drink.

Source:

<http://www.hattiesburgamerican.com/apps/pbcs.dll/article?AID=/20071115/NEWS01/71115021/1002>

[\[Return to top\]](#)

Public Health and Healthcare Sector

20. *November 16, News Tribune* – (National) **Experts reassure on cold virus strain.**

Reports of a cold virus that has killed 10 people nationwide are not cause for general concern, health experts say. The virus – known as adenovirus 14 – is “not a broad public health threat at this time,” a Centers for Disease Control expert on respiratory viruses said, adding that the flu is much more of a threat. His comments came after the CDC reported that adenovirus 14 might be linked to the deaths of seven people in Oregon, one in Texas, one in New York City and one in Washington State. The CDC official said Thursday’s report was mostly intended to remind medical providers that the virus can occasionally cause serious respiratory illness, so they should add it to their list of possible diagnoses.

Source: <http://www.thenewstribune.com/health/story/205276.html>

21. *November 15, Reuters* – (National) **Study shows how some AIDS vaccines may harm.**

After a study performed on lab mice, researchers from the Wistar Institute Vaccine Center in Philadelphia reported Thursday that some viruses being used in experimental AIDS vaccines may damage the immune system by exhausting key cells. They said vaccines using the viruses should not be tested on people until more studies are done. But other vaccine experts said the findings, while scientifically interesting, were not a cause for immediate alarm. The usually harmless adeno-associated viruses in question are used to carry genetic material from the AIDS virus into the body so that the immune system can recognize and rally against it. But the viruses themselves may be doing harm, said Wistar’s director. In mice, the viruses directly interfered with the very same T-cells the vaccine is supposed to activate in order to fight an HIV infection.

Source: <http://www.reuters.com/article/healthNews/idUSN1533549520071115?sp=true>

Government Facilities Sector

22. *November 16, The Record* – (New Jersey) **Gas leak empties high schools.** A gas leak at a New Jersey high school not only sent students home early on November 15, but triggered a temporary evacuation of another high school. Students and staff at Pascack Valley High School were evacuated about 10:20 a.m. after the head custodian informed the principal of an odor of gas in the building. When the source of the gas leak could not immediately be determined, the 1,130 students were sent home. Meanwhile, a Tenafly High School student received a text message from a phone number she did not recognize

that stated, “There is a gas leak in the school,” said the Tenaflly police captain. The student reported the message to school officials, prompting an evacuation of approximately 1,100 students. Students and staff were permitted to reenter the building about an hour later after no leak was discovered, he said. School officials later learned the text message was sent to the student by a friend who attends Pascack Valley. “As far as we now know, there was no attempt at causing a false alarm at the Tenaflly school. “It was an innocent mistake,” the police captain said. The Pascack Valley gas leak was located in the school’s basement and repaired.

Source:

<http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXk0NyZmZ2JlbDdmN3ZxZWVFRXl5NzIyMjA5NiZ5cmlyeTdmNzE3Zjd2cWVIRUV5eTQ>

23. *November 15, Associated Press* – (Florida) **3 accused of stealing from Air Force base for drug operation.** Three people have been charged with using chemicals and equipment from Tyndall Air Force Base to produce about \$300,000 worth of methamphetamine, Bay County, Florida, authorities said. One of those arrested told authorities he worked at the base as part of a cooperative partnership with North Carolina State University. A search of his car produced \$20,000 of chemicals and equipment believed to have been taken from the base, the *News Herald* of Panama City reported.

Source: <http://www.miamiherald.com/775/story/309641.html>

[\[Return to top\]](#)

Emergency Services Sector

24. *November 16, EMSResponder.com* – (National) **Recommendations and resources for dealing with MRSA.** In light of increasing national concern and media coverage over the spread of MRSA (methicillin-resistant *Staphylococcus aureus*), EMSResponder.com has compiled a list of online resources, and advice for EMS personnel. As MRSA continues to spread across the country, EMS personnel are encouraged to pay close attention to patients with open sores or wounds. Victims often include patients of health care facilities, high school athletes, rescue personnel and elementary school students. Some health officials are calling this spread of MRSA an epidemic, but careful hygiene may contain it. The public is advised to simply wash hands frequently with soap or an alcohol-based sanitizer, keep cuts and scrapes covered with a bandage and avoid sharing towels or other items. Health care providers should be especially diligent about wearing gloves and washing their hands after patient contact, and continue to use universal precautions, says the executive director of the Maryland Institute for Emergency Medical Systems (MIEMSS). “Other than the use of gloves and masks, there’s really nothing else we can suggest,” he said, but adding that particular attention should be taken if EMS personnel observe sores, boils or other injuries on their patients. Wounds should be covered. EMS agencies may also be able to improve their procedures and compliance for disinfecting vehicles and equipment, as outlined in this month’s EMS Magazine cover article, Bug Patrol. See <http://www.EMSResponder.com> for links and resources related to MRSA and infection control.

Source: <http://www.emsresponder.com/web/online/Top-EMS-News/MRSA-->

25. *November 14, San Jose Mercury News* – (California) **Drill snafu stirs concern.** An emergency drill in San Jose featuring a biological attack on a mock rock concert got a little too real today when a non-profit agency mistakenly sent out an e-mail warning members of a “public health emergency.” History San Jose, which sent the e-mail to its board members, corrected the mistake within about 25 minutes. But it touched off a flurry of calls between organizers of the drill and the non-profit. The development director of History San Jose, who issued the alert, said she was reacting to an advisory that came across the fax machine. She was puzzled about why History San Jose would receive the seemingly real warning that recommended that anyone who had been at the HP Pavilion in the past two days to seek medical treatment. A San Jose spokesman said the phony fax was sent to someone who was a dispatcher for the drill. But that fax machine is also used by History San Jose, which is located in a city building near where the drill was occurring. The faxed advisory read in part: “Officials have confirmed that Pneumonic Plague was released in HP Pavilion. Anyone who has been at the HP Pavilion within the past 2 days during the JamFest concert needs medication to prevent illness. Anyone who has come into direct contact with a concert attendee showing symptoms needs medication to prevent illness. A Medication Center is open at the SCC Fairgrounds. Surrounding cities have opened Medication Centers as well.” But it was just part of “Golden Guardian” drill where San Jose Municipal Stadium was doubling as HP Pavilion. Golden Guardian 2007 events occurred throughout the state Wednesday and included more than 3,000 players from 45 agencies including Anaheim, Orange County, Stockton and San Joaquin County. Created after the terrorist attacks of September 11, 2001, the drill is the largest state-sponsored, coordinated exercise in the nation.

Source: <http://www.emsresponder.com/online/article.jsp?siteSection=1&id=6566>

[\[Return to top\]](#)

Information Technology

26. *November 15, Army Times* – (Indiana) **Computer with veterans’ data stolen.** The Department of Veterans Affairs announced that a computer containing the names, Social Security numbers and birthdates of 12,000 veterans was taken over the Veterans’ Day weekend from the VA medical center in Indianapolis. Three computers were taken from an unlocked room, but one computer contained records that could be used for identity theft. The records are of veterans who had been treated as patients at the hospital. A policy established earlier this year calls for immediate notification of everyone whose information is missing and a review of the potential threat of identity theft in such situations. If there is a risk of identity theft, VA policy calls for the government to provide free credit monitoring to those affected. Federal, state and local law-enforcement agencies are investigating the theft.

-
27. *November 15, Computerworld* – (National) **What retail wireless security?** TJX may be

in a class all by itself in terms of the number of records compromised in a data breach. But the retailer apparently has plenty of company when it comes to wireless security issues of the sort that led to the compromise it disclosed earlier this year. A survey of over 3,000 retail stores in several major U.S. cities by wireless security vendor AirDefense Inc. reveals that a large number of retailers are failing to take even the most rudimentary steps for protecting customer data from wireless compromises. Among the biggest issues: weakly protected client devices, wrongly configured wireless access points inside stores, data leakage, poorly named network identifiers, and outdated access-point firmware. According to AirDefense, about 85 percent of the 2,500 wireless devices that it discovered in retail stores, such as laptops and barcode scanners, were vulnerable to wireless hacks. Out of the 4,748 access points that were monitored for the survey, about 550 had poorly named SSIDs that could give away the store's identity. "One thing we did not expect was the large number of point-of-sale devices that looked as if they had been turned on" and left in essentially the configuration in which they arrived at the store, said AirDefense's chief security officer. Many of the access IDs that were being used by retailers had names that were dead giveaways, such as 'retail wireless', 'POS WiFi' or 'store number 1234'," he said. About 25% of the access points that were monitored used no encryption at all. In total, of the 3,000 stores monitored, about a quarter of them were still using the Wired Equivalent Privacy (WEP) protocol for encrypting traffic. WEP is considered to be among the weakest of the encryption options available today and was the standard in use by TJX when it was first breached. Source:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9047258&taxonomyId=17&intsrc=kc_top

28. *November 15, Wired* – (National) **Hackers use banner ads on major sites to hijack your PC.** The worst-case scenario used to be that online ads are pesky, memory-draining distractions. But a new batch of banner ads is much more sinister: They hijack personal computers and bully users until they agree to buy antivirus software. And the ads do their dirty work even if you do not click on them. The malware-spiked ads have been spotted on various legitimate websites, ranging from the British magazine *The Economist* to baseball's MLB.com to the Canada.com news portal. Hackers are using deceptive practices and tricky Flash programming to get their ads onto legitimate sites by way of DoubleClick's DART program, which is used by Web publishers to manage advertising inventory. The ads work by closing a user's browser window from a legitimate Web site. A new browser window comes up, redirecting the user to an antivirus site, while a dialog box comes up claiming the computer is infected and that the hard drive is being scanned. The malware tries to download software to the computer and scans the hard drive again. The malware looks like an ordinary Flash file, with its redirect function encrypted, so that when publishers upload it, the malware is not detectable. Once deployed on a site, the Flash file launches the malicious redirects, which appear to be triggered at preset times or at selected Web domains. DoubleClick acknowledges the malware is out there, and says it has implemented a new security-monitoring system that has thus far captured and disabled a hundred ads. Publishers may be somewhat culpable, too. The distributor of the malware-infected ads is believed to be AdTraff, an online-marketing company with reported ties to the Russian Business

Network, a secretive internet service provider that, security firms say, hosts some of the internet's most egregious scams. AdTraff is believed to have posed as a legitimate advertiser, using its partners as references.

Source: <http://www.wired.com/techbiz/media/news/2007/11/doubleclick>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Communications Sector

29. *November 16, Business Wire* – (International) **Satellite industry safeguards C-band frequency spectrum use at WRC-07.** The global satellite industry emerged today from four weeks of successful negotiations to protect the users of its C-band spectrum from terrestrial interference. With its “no change” campaign, the satellite industry at the 2007 World Radiocommunication Conference (WRC-07) has ensured its uninterrupted, interference-free use of C-band for the future. “This outcome represents a strong endorsement by a large number of administrations of the critical nature and value of C-band satellite services as they exist today,” the CEO of SES NEW SKIES, an SES Company. The Chairman and CEO of Inmarsat, stated: [The] decision to protect the C-band will enable us to continue offering essential communications to mobile users where terrestrial networks cannot reach, including aeronautical and maritime safety services.” In addition to ensuring their uninterrupted use of the C-band, WRC-07 also gave satellite operators assurances that any future IMT (International Mobile Telecommunications) networks will provide them with full protection from interference. The endorsement of the satellite industry's use of this highly valuable spectrum in the band 3.4 - 4.2 GHz will ensure that operators will also have adequate bandwidth to roll out future service -- especially in those regions where they are most in demand. These include the developing world, large industrialized countries, and remote regions. The outcome, supporters said, showed recognition of the need for continued interference-free operation of C-band satellite services that are essential for the provision of national over-the-air and cable television services, emergency and disaster recovery communications, Internet services, and mobile and wireline telephony trunking services. Source: <http://www.broadcastnewsroom.com/articles/viewarticle.jsp?id=235276>

30. *November 16, RCR Wireless News* – (International) **700 MHz band to be used for broadband worldwide.** The United States teamed with neighboring countries to get the 700 MHz band identified for wireless broadband services in the Americas and major markets in Asia at the close of the World Radiocommunication Conference in Geneva, effectively setting the foundation for a global market for WiMAX services and products in frequencies being relinquished in various timeframes by broadcasters around the

globe. “WCA applauds a major victory for the broadband wireless industry in the agreement to adopt power limits on satellite services in the 2500-2690 MHz band that protects land-based services from interference in the major fourth generation/WiMAX frequency band in the U.S., and in many other parts of the world,” said the Wireless Communications Association International in a statement. Mobile satellite services armed with ancillary terrestrial component authorization won global recognition at WRC-07, but MSS-ATC will continue to lack the IMT imprimatur associated with 700 MHz and other frequency bands.

Source:

<http://www.rcrnews.com/apps/pbcs.dll/article?AID=/20071116/FREE/71116004/1005/allnews>

[\[Return to top\]](#)

Commercial Facilities Sector

31. *November 16, Associated Press* – (California) **Islamic school evacuated in scare.** A duffel bag left near the entrance of the Islamic school at the Islamic Center of Central Missouri in Columbia caused the evacuation of the school and several nearby businesses. School staff called police when they noticed that a male, who was “acting suspicious in the back lot,” had abandoned the bag there. It contained only paper and books, police said Thursday after blowing it up.

Source: [http://www.news-](http://www.news-leader.com/apps/pbcs.dll/article?AID=/20071116/NEWS01/711160373/1007/NEWS01)

[leader.com/apps/pbcs.dll/article?AID=/20071116/NEWS01/711160373/1007/NEWS01](http://www.news-leader.com/apps/pbcs.dll/article?AID=/20071116/NEWS01/711160373/1007/NEWS01)

[\[Return to top\]](#)

National Monuments & Icons Sector

32. *November 15, Associated Press* – (Minnesota) **Father, son allegedly cut trees in Chippewa National Forest.** A father and son have been indicted for allegedly cutting down trees in the northeast corner of Minnesota’s Chippewa National Forest for export. They are accused of removing or transporting timber from U.S. public lands; cutting or injuring timber; and theft of government property.

Source: <http://www.dglobe.com/ap/index.cfm?page=view&id=D8SUCFHO2>

33. *November 15, Associated Press* – (National) **Energy corridors proposed across public lands in West.** The Bush administration is proposing more than 6,000 miles of “energy corridors” for future pipelines and transmission lines in the West, crossing dozens of sensitive areas including national monuments, recreation areas, and scenic rivers. Federal officials say the 3,500-foot-wide corridors are needed to keep pace with the electricity demands of a swelling population and the region’s increasing oil and gas production. The plan, developed over two years, would affect federal lands in 11 western states. It was released November 8 by the Departments of Interior, Energy, Agriculture, Commerce, and Defense. Environmental groups say the plan would allow industrial projects to be carved through some of the most scenic open lands in the country, although they concede that the draft plan was an improvement over prior

versions. In the latest draft, for example, the number of national parks, monuments and recreation areas crossed dropped from 29 to 12. The number of national wildlife refuge crossings dropped from 15 to 3. An employee of the federal Bureau of Land Management, one of the lead agencies involved, said it was impossible to avoid environmentally sensitive areas altogether. But by designating corridors, she said, the government hoped to “bundle future projects so they’re not totally scattered across the landscape.” Almost two-thirds, or about 3,700 miles, are proposed along existing roads or utility right of ways. Those would be widened in many cases to allow for a dramatic expansion of infrastructure, as many as nine large transmission lines or 29 natural gas pipelines in each corridor.

Source: <http://www.azcentral.com/news/articles/1115energy-corridors1115-ON.html>

[\[Return to top\]](#)

Dams Sector

34. *November 16, Appeal-Democrat* – (California) **Doubt shrouds flood-protection system at Sutter site.** The U.S. Army Corps of Engineers will investigate whether a flood-protection system at one of Sutter County, California’s, most trouble-prone levee spots is working right. Corps-installed relief wells are supposed to drain a Feather River levee of high-pressure water that could threaten the levee during a flood. But worrisome boils popped up near the system during a relatively minor storm almost two years ago, casting doubts on whether it is functioning properly. “They’ll take a quick look at the wells, probably talk to the levee district,” said a Corps spokesman. So far, it appears that two of the 12 relief wells may not be working properly and may be pulling water from outside of the well casing rather than inside.

Source:

http://www.appeal-democrat.com/news/levee_56539_article.html/wells_flood.html

35. *November 15, University of Missouri* – (National) **MU engineers designing sensor system to prevent dam failure.** A professor of civil and environmental engineering at the University of Missouri’s College of Engineering is developing a sensor system that will remotely measure how much strain is being placed on a type of spillway gate called a Tainter gate. Indirectly, the sensors will measure the condition of the gate’s hinge – a known problem area that is not only difficult to reach, but hidden within the gate’s construction. The professor received \$48,108 from the U.S. Army Corps of Engineers to develop and test the Tainter gate monitoring system. The monitoring project targets the curved metal gate’s hinges – its trunnion bearings, specifically – which are susceptible to corrosion, but cannot be easily removed for inspection. In 1995, a Tainter gate on Folsom Dam in California broke suddenly, releasing a torrent of water into the Lower American River. While no one was injured by the flood, the accident prompted federal engineers to review Tainter gate design, according to a civil engineer in charge of the project for the Corps’ Engineer Research and Development Center. The Tainter gate monitoring system will be tested next spring at the Carlyle Lake Dam in Illinois. Once proven, the Corps plans to use the Tainter gate monitoring system as a portable measurement system at similar dams throughout the country.

Source: <http://www.physorg.com/news114358341.html>

36. *November 15, KSBY 6 Santa Barbara* – (California) **Preparing for disaster: Local agencies mock massive flooding at Twitchell Dam.** In Santa Maria, California, several agencies practiced what to do in case massive flooding hit the Twitchell Dam. In a normal season, it takes about 12 to 14 inches of rain before any water is seen in the reservoir. The last time it came close to overflow levels was in 1998, during the El Nino season. With the upcoming rainy season, the city may have increased runoff, thanks to the Zaca Fire, which charred some of the region’s watershed, creating the danger of increased runoff from burned areas. City officials say the blaze charred about seven percent of the watershed which feeds into the Twitchell Reservoir. “There is a heightened threat from the Zaca fire, certainly, both of those watersheds cover a huge area of land,” said a management analyst for the city of Santa Maria. As far as repairing the burned watershed area, city officials say that is up to the Los Padres National Forest. Among the groups participating were the Bureau of Reclamation, the U.S. Army Corps of Engineers, as well as a number of city and county agencies.
Source: <http://www.ksby.com/Global/story.asp?S=7368614>

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCRports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389
Subscription and Distribution Information:	Send mail to NICCRports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

